# CRYPTOGRAPHIC SYSTEM AND METHOD WITH KEY ESCROW FEATURE

**Publication number:** EP0739560
**Publication date:** 1996-10-30
**Inventor:** SUDIA FRANK W (US)
**Applicant:** BANKERS TRUST CO (US)
**Classification:**
**- international:** ***G06Q20/00; G09C1/00; H04L9/08; H04L9/32;*** *G06F7/72;* **G06Q20/00; G09C1/00; H04L9/08; H04L9/32;** G06F7/60; (IPC1-7): H04L9/08; H04L9/32
**- european:** G06Q20/00K1; H04L9/08; H04L9/08R; H04L9/32
**Application number:** EP19950908511 19950113
**Priority number(s):** US19940181859 19940113; US19940272203 19940708; WO1995US00531 19950113

**Also published as:**
WO9519672 (A3)
WO9519672 (A2)
EP0739560 (A3)
US6009177 (A1)
US5872849 (A1)
more >>

**Report a data error here**

Abstract not available for EP0739560
Abstract of corresponding document: **US5841865**

The invention provides a cryptographic system and method with a key escrow feature that uses a method for verifiably splitting users' private keys into components and for sending those components to trusted agents chosen by the particular users, and provides a system that uses a modern public key certificate management, enforced by a chip device that also self-certifies. A preferred embodiment of this invention provides a method for generating verifiably trusted communications among a plurality of users, comprising the steps of escrowing at a trusted escrow center a plurality of asymmetric cryptographic keys to be used by a plurality of users; verifying each of said plurality of keys at the escrow center; certifying the authorization of each of said plurality of keys upon verification; and initiating a communication from each of said plurality of users using a respective one of said plurality of keys contingent upon certification. Further preferred embodiments provide for rekeying and upgrading of device firmware using a certificate system, and encryption of stream-oriented data.

Data supplied from the ***esp@cenet*** database - Worldwide